

UNITED STATES DISTRICT COURT
 for the
 District of Oregon

In the Matter of the Search of

(Briefly describe the property to be searched
 or identify the person by name and address)

)
)
)

Case No. 3:24-mc-1189 A-B

A dark blue Samsung cell phone and Alfredo
 Terrero-Ortega Buccal Swabs (DNA Sample) as
 described in Attachments A-1 and A-2

)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A dark blue Samsung cell phone and Alfredo Terrero-Ortega Buccal Swabs (DNA Sample) as described in Attachments A-1 and A-2 hereto,

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachments B-1 and B-2 hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 922(g)(1);	Felon in Possession of a Firearm;
18 U.S.C. § 924(c)(1)(A)	Possession of a Firearm in furtherance of a Drug Crime

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 Robert Krause, DUSM

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 Telephone at 4:28 pm a.m./p.m. (specify reliable electronic means).

Date: November 14, 2024

Youlee Yim You

 Judge's signature

City and state: Portland, Oregon

Hon. Youlee Yim You, United States Magistrate Judge

Printed name and title

ATTACHMENT A-1

Property to Be Searched

The item to be searched is a dark blue Samsung cell phone with
“IMEI:350963863654021” printed on the back currently secured in USMS Evidence room
located within room 240.28 of suite 240 on the 2nd floor of the Mark O. Hatfield Federal
Courthouse, located at 1000 SW 3rd Ave, Portland, OR 97204. See pictures below:



ATTACHMENT A-2

Person to Be Searched

The person to be searched is Alfredo TERRERO-ORTEGA, a male, date of birth 09/16/1997, FBI number 635145PD8, currently in custody at the Washington County Jail located at 215 SW Adam's Avenue, Hillsboro, Oregon, 97123. TERRERO-ORTEGA is listed as five feet, seven inches, and 200 pounds. In his photograph, TERRERO-ORTEGA has brown eyes and black hair. See the photograph, below:



ATTACHMENT B-1**Items to Be Seized**

1. The items to be searched for, seized, and examined, are those items on **Target Cell Phone**, as described in Attachment A-1, that relate to violations of 18 U.S.C. § 922(g)(1), felon in possession of a firearm, and 18 U.S.C. § 924(c)(1)(A), possession of a firearm in furtherance of a drug crime, including:

- a. Evidence related to the possession of firearms and firearm accessories;
- b. Evidence of drug crimes involving TERROR-ORTEGA;
- c. Evidence indicating how and when the **Target Cell Phone** was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the **Target Cell Phone** owner;
- d. Records relating to who created, used, or communicated with the user ID including records about their identities and whereabouts;
- e. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

2. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

/ / /

/ / /

Search Procedure

3. Law enforcement may press the fingers, including thumbs, of TERRERO-ORTEGA to the sensors of the **Target Cell Phone** for the purpose of attempting to unlock the device via biometric authentication. Further, law enforcement is authorized to point the camera of the **Target Cell Phone** at the face of TERRERO-ORTEGA for the purpose of attempting to unlock the device via biometric authentication.

4. The examination of the Device, as described in Attachment A-1, may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

5. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file

system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and it is determined that a Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

8. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

a. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

ATTACHMENT B-2

Items to Be Seized

1. The items to be searched for, seized, and examined, are on the person of Alfredo TERRERO-ORTEGA, and buccal swabs (DNA sample) to be taken from TERRERO-ORTEGA, that contain evidence of violations of 18 U.S.C. § 922(g)(1), felon in possession of a firearm, and 18 U.S.C. § 924(c)(1)(A), possession of a firearm in furtherance of a drug crime, including:
 - a. DNA standard by obtaining swabs from the interior of TERRERO-ORTEGA's cheek. These swabs are to be collected by the USMS and any designated Deputies or Officers.

DISTRICT OF OREGON, ss:

AFFIDAVIT OF ROBERT KRAUSE

**Affidavit in Support of an Application
Under Rule 41 for Search Warrants**

I, Robert Krause, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Criminal Investigator Deputy United States Marshal (CIDUSM) with the United States Marshals Service and have been since April of 2022. I am responsible for conducting fugitive investigations that result in arrest and prosecutions of individuals who are facing criminal charges in state and federal court. As a Criminal Investigator Deputy U.S. Marshal, I am authorized under 28 U.S.C. § 564 to enforce the federal criminal laws of the United States. My training and experience include completion of the Federal Criminal Investigator Training Program and the U.S. Marshals Service Basic Academy at the Federal Law Enforcement Training Center in Glynco, Georgia. I have also attended additional training provided by other law enforcement entities relating to fugitive and criminal investigations.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search:

- a. a dark blue Samsung cellphone with “IMEI:350963863654021” printed on the back (hereinafter “**Target Cell Phone**”) currently secured in USMS Evidence room located within room 240.28 of suite 240 on the 2nd floor of the Mark O. Hatfield Federal Courthouse, located at 1000 SW 3rd Ave, Portland, OR 97204;

///

///

Affidavit of Robert Krause

Page 1

b. the person of Alfredo TERRERO-ORTEGA (hereinafter “TERRERO-ORTEGA”) a male, born in 1997¹, currently being held in custody at the Washington County (OR) Jail located at 215 SW Adams Ave, Hillsboro, OR 97123;

as described in Attachment A-1 and A-2 for evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 922(g)(1), felon in possession of a firearm, and 18 U.S.C. § 924(c)(1)(A), possession of a firearm in furtherance of a drug crime. As set forth below, I have probable cause to believe that such property and items, as described in Attachment B-1 and B-2 hereto, including any digital devices or electronic storage media are located inside the **Target Cell Phone** and TERRERO-ORETGA.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offenses

4. I believe there is probable cause to believe that evidence of the crime of Felon in Possession of a Firearm (18 U.S.C. § 922(g)(1)) and Possession of a Firearm in Furtherance of a

¹ I know the exact date of birth, but I am omitting it in this document to protect the personal identifying information of a third party because this document will be public record at some point.

Drug Crime (18 U.S.C. § 924(c)(1)(A)) will be found in the **Target Cell Phone** and TERRERO-ORTEGA.

Statement of Probable Cause

5. According to criminal history records, on January 23rd, 2018, Alfredo TERRERO-ORTEGA was sentenced in Washington County (OR) Circuit Court on case 17CR70475 to 18 months and 20 months imprisonment with the Oregon Department of Corrections for convictions of Sexual Abuse in the Second Degree and Criminal Mistreatment in the First Degree. On February 1st, 2019, Alfredo TERRERO-ORTEGA was sentenced in Washington County (OR) Circuit Court on case 18CR63054 to 35 months and 60 months imprisonment with the Oregon Department of Corrections for convictions of Attempt to Commit a Class A Felony and Unlawful Use of a Weapon with a Firearm. On July 5th, 2023, an arrest warrant for parole violation was issued by the Oregon State Parole Board. Based on this history, I believe TERRERO-ORTEGA qualifies as a felon under federal law.

6. On Thursday, November 7th, 2024, I was assisting Task Force Officers (TFOs) with the attempted apprehension of Alfredo TERRERO-ORTEGA on the above-mentioned parole violation warrant. The operation was being led by TFO NICHOLS of the Washington County Sheriff's Office. As part of the briefing, TFO NICHOLS distributed TERRERO-ORTEGA's criminal history and information that he was residing at 36xx NE Mallory Ave #1xx², Portland, OR. TFO NICHOLS also provided information to Task Force Officers from Adult 1 (I know the identity of Adult 1, but I have omitted their name from this affidavit in order to protect their privacy), who is familiar with TERRERO-ORTEGA. Adult 1 provided the

² I am aware of the full address, but I have redacted it partially here because third parties reside at this location, and I do not want to disclose this personal identifying information in a document that will be publicly viewable.

following information on the same day, just hours before TERRERO-ORTEGA's arrest.

According to Adult 1, TERRERO-ORTEGA often carries a black satchel bag with him whenever he is in public, and the black satchel bag contains a handgun.

7. It should be noted for the Court's consideration, a search of Adult 1's criminal history revealed no arrests and/or convictions for crimes involving lying, false statements, fraud, ID theft, perjury, theft, or any other crimes exhibiting a potential history or pattern of deception.

8. At approximately 12:20 pm, Thursday, November 7th, 2024, TFO DELONG positively identified TERRERO-ORTEGA as a subject wearing a blue jacket and blue baseball hat, carrying a black satchel bag in his left hand, while walking southbound on NE Martin Luther King (MLK) Jr Blvd, near NE Morris St, in Portland, OR. Task Force Officers responded to the area and at approximately 12:30 pm approached TERRERO-ORTEGA by foot and vehicle near the intersection NE MLK Jr Blvd and NE Graham St. Due to the credible information of TERRERO-ORETGA likely carrying a handgun, a flash sound diversionary device was deployed by Task Force Officers during approach. TFO ATKINS was one of the first officers to approach TERRERO-ORTEGA and said that he saw TERRERO-ORTEGA dropped the black satchel bag onto the sidewalk when the flash sound diversionary device was deployed. Task Force Officers were able to quickly apprehend TERRERO-ORTEGA and DUSM FITZPATRICK immediately took possession of the black satchel bag. DUSM FITZPATRICK handed the black satchel bag to TFO NICHOLS who secured it in TFO SCHNACKENBERG's vehicle.

9. During the arrest, but prior to advising TERRERO-ORTEGA of his *Miranda* rights, TFO NICHOLS asked him what property belonged to him and what was inside the satchel. TERRERO-ORTEGA replied, you guys know what's in the bag. Later, I advised

TERRERO-ORTEGA of his *Miranda* rights, and he indicated he understood. I asked him what was inside the satchel, and he gave essentially the same response – you already know what's in the bag. I believe, based on my training and experience, that TERRERO-ORTEGA was aware that the satchel contains contraband and was being evasive with his answers.

10. At approximately 12:45 pm, I took possession of the black satchel bag from TFO SCHNACKENBERG, at his vehicle, while still on scene of the arrest. As I was handed the bag, I could feel a heavy rigid object resting near the bottom of the bag. Based on my training and experience, the weight and feel of the black satchel bag resting in my hand was consistent with the feel of a bag containing a handgun.

11. I secured the black satchel bag in my vehicle and it remained in my custody until it was lodged into the USMS Evidence room, located within room 240.28 of suite 240 on the 2nd floor of the Mark O. Hatfield Federal Courthouse - 1000 SW 3rd Ave, Portland, OR 97204 - at approximately 2:45 pm, Thursday, November 7th, 2024.

12. On Friday, November 8th, 2024, the Honorable Jeffery Armistead signed a search warrant for the black satchel bag carried by TERRERO-ORTEGA during his arrest on November 7th, 2024 (3:24-mc-1170). On Tuesday, November 12th, 2024, I executed the search warrant in the presence of TFO DELONG and Portland Police Bureau Criminalist GREAVES in the Portland Police Bureau forensic lab, located at 1111 SW 2nd Avenue room 1250, Portland, OR 97204. Amongst other personal belongings, the following noteworthy items were located inside the bag:

- a. a loaded black Beretta APX 9mm handgun (serial number: AXC049108) with one round in the chamber and three in the magazine;

- b. a dark blue Samsung cellphone with "IMEI:350963863654021" printed on the back (**Target Cell Phone**);
- c. eight assorted small and mini sized Ziploc style baggies contained within a black coin pouch;
- d. two medium sized Ziploc style baggies with a clear crystal-like substance inside;
- e. one glass tube with a bulbous end and two broken glass tubes with a white substance coating inside.

13. The black Beretta APX handgun was swabbed for DNA evidence by Criminalist GREAVES (PPB Case 24-680740). I later secured the DNA swabs and lodged them into the USMS Evidence room within room 240.28 of suite 240 on the 2nd floor of the Mark O. Hatfield Federal Courthouse, located at 1000 SW 3rd Ave, Portland, OR 97204 on Tuesday November 12th, 2024. Based on my training and experience, I am aware that if TERRERO-ORTEA's DNA is collected, it can be analyzed and compared to DNA samples collected from the items of evidence.

14. I separately placed the two medium sized Ziploc style baggies containing a clear crystal-like substance on a scale and observed a weight of 3.0 and 1.9 grams. I conducted a NIK test of the contents of each bag and observed a presumptive positive result for methamphetamine.

15. Based on my training and experience, I know that distributors of user quantities of narcotics often utilize small and mini sized Ziploc style baggies to package their product. These user quantities of narcotics are often sourced from a larger storage container(s) in the distributors immediate or constructive possession. Distributors of narcotics often use cell phones to coordinate and record their narcotics transactions. They will also store contact information for

suppliers and customers on their cell phones for quick identification and use. Additionally, I know that distributors of narcotics will often carry firearms to protect themselves, their product, and their drug proceeds from potential theft or robbery attempts.

16. Based on the above listed contents of the black satchel bag, I believe TERRERO-ORTEGA both uses and distributes methamphetamine. I believe the crystal-like substance in the two medium sized Ziploc style baggies, which returned a presumptive positive result for methamphetamine, together with the 8 small/mini size Ziploc style baggies, close in proximity to the loaded firearm, are evidence of drug distribution and possession of a firearm in furtherance of drug trafficking.

17. Based on my training and experience, I believe the contents of the **Target Cell Phone** will possess information establishing TERRERO-ORTEGA as the user of this device. Given that the Device was in the same satchel as the firearm, I believe evidence connecting him to the Device will help establish his knowing possession of the firearm. I also believe the Target Cell Phone will contain evidence of recent narcotic distribution activity by TERRERO-ORTEGA.

Electronic Device Information

18. Based on my training and experience, a cellphone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address

books;” sending, receiving, and storing text messages and email; taking, sending, receiving and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet, including the use of apps. Wireless telephone may also include global positioning system (“GPS”) technology for determining the location of the device.

19. Based on my training and experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggest who possessed or used the phone, how the phone was used, the purpose of its use, and locations of evidentiary value to the investigation.

20. As further described in Attachment B-1, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

- a. Phones can store information for long periods of time, including information viewed via the internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a

file, the data contained in the file does not actually disappear, rather that the data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the phone that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

- b. Wholly apart from user-generated files, the Devices may contain electronic evidence of how they have been used, what they have been used for, and who has used them. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.
- c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- d. Data on the Devices can provide evidence of a file that was once on the Devices but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Devices that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Devices that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the Devices was in use. File

systems can record information about the dates files were created and the sequence in which they were created.

- e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- f. A person with appropriate familiarity with how the Device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Device was used, the purpose of their use, who used them, and when.
- g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Device is evidence may depend on other information stored on the Device and the application of knowledge about how a Device functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- h. Further, in order to find evidence of how the Device was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the Device.

Nature of Examination

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Device and

computer-assisted scans and searches of the entire Device that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

22. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

23. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

24. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

/ / /

/ / /

25. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

26. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Manner of Execution

27. Because this warrant seeks only permission to examine devices once in law enforcement's possession, the execution of the **Target Cell Phone** warrants do not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the **Target Cell Phone** warrant at any time in the day or night.

Requirement to Access Device(s)

28. I know from my training and experience, as well as from information found in publicly available materials that some digital devices offer their users the ability to unlock the device via the use of a fingerprint, thumbprint, or facial recognition in lieu of a numeric or alphanumeric passcode or password. These features are commonly referred to as "biometric authentication" and their availability is dependent on the model of the device as well as the operating system on the device. If a user enables biometric authentication on a digital device, he or she can register their fingerprints or facial biometric pattern and data to unlock that device.

29. In some circumstances, biometric authentication cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) too many unsuccessful attempts to unlock the device via biometric authentication are made; (4) when too many hours have passed since the last time the device was unlocked; and (5) when the device has not been unlocked via biometric authentication for a period of time and the passcode or password has not been entered for a certain amount of time. Thus, in the event law enforcement encounters a locked digital device, the opportunity to unlock the device via biometric authentication exists only for a short time.

30. The passcode or password that would unlock the **Target Cell Phone** are not known to law enforcement. Thus, it will likely be necessary to press the finger of only TERRERO-ORTEGA to **Target Cell Phone** or allow **Target Cell Phone** to read his facial biometric pattern in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via biometric authentication is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

31. I therefore request the Court to authorize law enforcement to press the fingers, including thumbs, of only TERRERO-ORTEGA to the sensor of **Target Cell Phone**, or on the person of TERRERO-ORTEGA, for the purpose of attempting to unlock the device(s) via biometric authentication. Further, I request that the Court authorize law enforcement to point the camera of the device suspected to be the **Target Cell Phone** at the face of only TERRERO-ORTEGA for the purpose of attempting to unlock the device via biometric authentication.

/ / /

Conclusion

32. Based on the foregoing, I have probable cause to believe, and I do believe, that Alfred TERRERO-ORTEGA committed Unlawful Acts, 18 U.S.C. § 922(g)(1), felon in possession of a firearm, and 18 U.S.C. § 924(c)(1)(A), Possession of a Firearm in Furtherance of a Drug Crime, and that evidence of that offense, as described above and in Attachment B1 and B2, are presently located in the property and person, which is described above and in Attachment A1 and A2. I therefore request that the Court issue a warrant authorizing a search of the property and person described in Attachment A1 and A2 for the items listed in Attachment B1 and B2 and the seizure and examination of any such items found.

33. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Leah K. Bolstad. I was informed that it is AUSA Bolstad's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone pursuant to Fed. R. Crim. P. 4.1
ROBERT KRAUSE
Deputy, US Marshals Service

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at
4:28 pm a.m./p.m. on November 14, 2024.

Youlee Yim You
HONORABLE YOULEE YIM YOU
United States Magistrate Judge